

Attorney Docket No. 16869P-097900US  
Client Ref. No. 340300055US1

# **PATENT APPLICATION**

## **POLICY SETTING SUPPORT TOOL**

**Inventors:** **Masato ARAI**  
Citizenship: Japan

**Satoshi KAI**  
Citizenship: Japan

**Assignee:** **Hitachi, Ltd.**  
6, Kanda Surugadai 4-chome  
Chiyoda-ku, Tokyo, Japan  
Incorporation: Japan

**Entity:** **Large**

**TOWNSEND AND TOWNSEND and CREW LLP**  
Two Embarcadero Center, 8th Floor  
San Francisco, California 94111-3834  
(415) 576-0200

## TITLE OF THE INVENTION

ポリシー設定支援ツール (Policy Setting Support Tool)

## BACKGROUND OF THE INVENTION

本発明は、コンピュータシステムが管理する情報資産に対するアクセスを、所定のポリシーに基づいてコントロールするアクセス制御システムに用いるポリシー設定支援ツールに関する。

一般のコンピュータシステムでは、マルチユーザマルチタスクOSが備えるユーザ認証機構と、該認証結果に基づいたアクセス制御機構を用いて情報その他コンピュータ資源の保護を実現しているケースが多い。具体的には、上記OSが実装された情報処理装置を利用する際に、ユーザは必ず自己のユーザIDとパスワードを入力し、認証を受ける。

上記情報処理装置が管理する全てのファイル各々には、ファイル読み出しや書き込み等のアクセスタイプ毎に、ユーザIDとグループIDを用いてアクセス可能なユーザを定義したアクセスコントロールリスト（ポリシーと称す）がセキュリティ属性情報として割り当てられている。

ユーザがアプリケーションプログラムを介してファイルへアクセスした場合、上記OSは、アクセス要求元となるユーザのID及び該ユーザが所属するグループのIDを、アクセス対象となるファイルやディレクトリに割り当てられたポリシーと照合し、当該リストに上記ユーザが含まれている場合に限りアクセスを許可するといった制御を行う。

また、アクセス要求元の情報として、上記ユーザIDやグループIDだけでなく、例えばアクセス手段となるプログラムの識別子まで確認すれば、より厳密なアクセス制御が可能となる。

このようなアクセス制御の方法は、例えば Japanese Laid Open Patent Publication No. 2001-337864（文献1）に開示されている。ただし、不正アクセスを防止するには、本来の利用目的であるサービス提供や業務遂行の上で必要最小限のアクセスのみ許可されるよう、上記ポリシーを設定しておくことが重要である。

その他、Japanese Laid Open Patent Publication No. 2002-108818（文献2）には、セキュリティポリシーの作成に要する時間を短縮するために、複数の雛形のポリシーから自己に見合ったものを選択し、修正しながらポリシーを作成する方法が開示されている。

先に述べたように、情報資産を安全に利用するためには、当該情報への必要最小限のアクセスのみ許可するようにポリシーを定義することが重要である。しかし、ユーザIDやグループIDだけでなく、アクセス手段となるプログラムの識別子まで組み合わせてポリシーを定義することは、厳密なアクセス権チェックができる代わりに、そのポリシー作成に手間がかかる。例えば、どのようなデータにアクセスするかといったソフトウェアの仕様を知らなければ、適切なポリシーは設定できない。

ソフトウェアが複数のプログラムから構成されている場合は、特に難しいと言える。上記文献2に記載されている方法を用いても、雛形のポリシーを自己に見合ったものに修正するのは全て利用者自身であるため、ソフトウェアの仕様を知らなければ、どこをどのように修正すべきか判断できないケースも発生し得る。

また、プログラムアップデートによるプログラムファイル自体の変更が発生したり、ユーザやグループの登録内容に変更が発生したり、更には情報資産であるファイルやディレクトリが、削除・移動・名称書き換え等により変更されることで、現在のポリシーの記述と一致しなくなれば、適切なアクセス制御ができなくなるという問題もある。

## SUMMARY OF THE INVENTION

本発明は、利用するソフトウェアの仕様を知らなくても、コンピュータの利用目的を果たす上で適切なファイルアクセスのみを許可するようにポリシーを設定可能な、ポリシー設定支援ツールを提供する。

本発明は、アクセス主体となるユーザやプログラムの情報の他、アクセス対象となるファイルやディレクトリ等に変更があった場合でも、簡易な操作により関連するポリシーの設定内容を更新可能な、ポリシー設定支援ツールを提供する。

本発明は、コンピュータが管理する資産をポリシー情報に基づいてアクセス制御する機構を備えたコンピュータシステムにおいて、上記ポリシー情報の作成に要する作業負担を軽減するためのポリシー設定支援ツールであって、当該ポリシー設定支援ツールは、アクセス主体となるサブジェクトの種類毎に用意した情報と、アクセス対象となるオブジェクトの種類毎に用意した情報から、適切なポリシーを作成するものであり、上記サブジェクトの種類毎に用意した情報とは、サブジェクトの種類毎に標準的あるいは推奨のポリシーを記述したサンプル情報と、サブジェクトの正常な動作を記録したアクセスログ情報と、対象のコンピュータシステムにインストールされているサブジェクトのインストール先パス名を含むインストール情報とからなり、上記オブジェクトの種類毎に用意した情報とは、オブジェクトの種類毎にアクセス手段として利用される頻度の高いサブジェクトの情報を記述した関連付け情報とからなり、更に上記ポリシー設定支援ツールは、上記サブジェクトの動作を監視して上記アクセスログ情報に記録するためのアクセス監視部と、上記サンプル情報と上記インストール情報とを照合して差分を検出する差分検出部と、上記サンプル情報と上記関連付け情報と上記差分検出部による検出結果とからポリシーの原案を作成するポリシー生成部と、ポリシーの原案を表示して利用者による更なるポリシーの修正および保存をするためのユーザインタフェース部とから構成されることを特徴としている。

上記ポリシー設定支援ツールによれば、例えばソフトウェアの種類毎にサンプルとなるポリシーが提供され、且つ対象のコンピュータシステムに適合したポリシーの原案まで自動的に作成できるので、利用者はソフトウェアの仕様を知らなくても、適切なポリシーが容易に設定可能となる。

また、本発明は、上記ポリシー設定支援ツールにおいて、当該ポリシー設定支援ツールの利用者は、上記ユーザインタフェース部を通じて、上記サンプル情報と、上記関連付け情報と、上記アクセスログ情報とから、1つ以上の情報を用いてポリシーの原案を作成し、当該ポリシー原案を元に必要に応じて更に修正を加え、修正後のポリシーを保存することで、上記ポリシー情報を設定することを特徴としている。

これにより、上記サンプルとなるポリシーが用意されていない場合でも、上記関連付け情報やアクセスログ情報からポリシーの原案が作成できるので、利用者はソフトウェアの仕様を知らなくても、適切なポリシーが容易に設定可能となる。

また、本発明は、コンピュータが管理する資産をポリシー情報に基づいてアクセス制御する機構を備えたコンピュータシステムにおいて、上記ポリシー情報の維持に要する作業負担を軽減するためのポリシー設定支援ツールであって、アクセス対象となるオブジェクトならびにアクセス主体となるサブジェクトに関する最新情報と、当該最新情報と設定済みのポリシーの内容とを照合しながら更新すべき項目を検出するための差分検出部と、当該差分検出部による検出結果の表示処理と、利用者による目視確認および上記ポリシーの更新処理をするためのユーザインタフェース部とから構成されることを特徴としている。

これにより、アクセス主体となるサブジェクトの情報や、アクセス対象となるオブジェクトに変更があった場合でも、更新すべき項目を自動的に検出して表示できるので、簡易な操作で関連するポリシーの更新が可能となる。

また、本発明は、上記ポリシー設定支援ツールにおいて、上記差分検出部による検出処理は、定期的に、あるいは利用者からの要求を受けた時点で実行されるものであり、差分を検出した場合には、当該差分情報を、上記ユーザインタフェース部を通じて利用者向けに表示し、上記ポリシー設定支援ツールの利用者は、上記ユーザインタフェース部を通じて表示される上記差分情報を目視で確認し、当該表示通りに更新すべきかどうかを判断し、更新すべきであれば上記ユーザインタフェース部を通じて必要な修正を加えた上で、上記ポリシー情報を保存することを特徴としている。

これにより、利用者は上記ユーザインタフェース部を通じて、差分情報の確認と、ポリシーの修正および保存まで、ポリシーの更新に必要な処理を全て行うことができる。

また、定期的な差分検出処理も可能とすることで、利用者が自ら上記差分検出部に対して要求を出さなくても差分情報を取得できるようになるため、無効なポリシー記述を放置することなく、常に適切なポリシーに基づくアクセス制御が可能となる。

また、本発明は、コンピュータが管理する資産をポリシー情報に基づいてアクセス制御する機構を備えたコンピュータシステムにおいて、上記ポリシー情報の作成に要する作業負担を軽減するためのポリシー設定支援ツールであって、上記コンピュータシステムは、アクセス対象となるオブジェクトの種類毎にアクセス手段として利用される頻度の高いサ

プロジェクトの情報を記述した関連付け情報を備えており、上記ポリシー設定支援ツールは、上記関連付け情報からポリシー情報を作成することを特徴としている。

このようにオブジェクトの種類毎にアクセス可能なサブジェクトを決定することで、ポリシー情報の設定が容易になるだけでなく、各オブジェクトの移動やコピー、削除が発生しても、同一種類のオブジェクトである限り同一のポリシー情報に基づくアクセス制御が可能となり、ポリシー情報の変更が不要となる。

また、本発明は、上記ポリシー設定支援ツールにおいて、オブジェクトへのアクセス手段を用途別に指定するための用途別サブジェクト指定手段を備えており、当該用途別サブジェクト指定手段を利用して指定されたプログラムであれば、複数種類のオブジェクトに関連付けられたサブジェクトとして上記ポリシー情報を作成することを特徴としている。

これにより、関連付け情報のみを用いた場合よりも、柔軟なポリシー情報が設定可能になるとともに、上記ポリシー設定支援ツールと同様に、各オブジェクトの移動やコピー、削除が発生しても、同一種類のオブジェクトである限りポリシー情報の変更は不要となる。

また、本発明のポリシー設定支援ツールは、上記ポリシー情報に違反するアクセスが発生した場合に上記アクセス制御機構から通知を受けて、当該アクセスの対象となるオブジェクトを管理するコンピュータシステムの利用者に対してメッセージを伝え、上記利用者による判断に基づいて所定の処理を実行する手段を備えており、上記利用者による判断とは、上記ポリシー違反のアクセスを以後全て許可するか、今回のアクセスのみ許可するか、禁止するかのいずれかであり、上記ポリシー違反のアクセスを以後全て許可する場合には、上記ポリシー設定支援ツールによる所定の処理として上記アクセスが正当なアクセスとなるようポリシー情報を変更し、上記アクセス制御機構に対しては上記アクセスが正当であることを通知し、上記ポリシー違反のアクセスを今回のみ許可する場合には、所定の処理として上記ポリシー情報は変更せず、上記アクセス制御機構に対しては上記アクセスが正当であることを通知し、上記ポリシー違反のアクセスを禁止する場合には、所定の処理として上記ポリシー情報は変更せず、上記アクセス制御機構に対しては上記アクセスが不正であることを通知することを特徴としている。

更に、上記ポリシー設定支援ツールは、上記ポリシー情報に登録されていない新種のオブジェクトに対して、当該オブジェクトに関連付けられたサブジェクトからアクセスが発生した時に、上記アクセス制御機構から通知を受け、上記コンピュータシステムの利用者に対してメッセージを伝え、上記利用者による判断に基づいて所定の処理を実行する手段を備えており、上記利用者による判断とは、新種のオブジェクトに対する当該オブジェク

トに関連付けられたサブジェクトからのアクセスを許可するか、禁止するかのいずれかであり、上記アクセスを許可する場合には、上記ポリシー設定支援ツールによる所定の処理として上記アクセスが正当なアクセスとなるようポリシー情報を変更して、上記アクセス制御機構に対しては上記アクセスが正当であることを通知し、上記アクセスを禁止する場合には、上記ポリシー情報は変更せず、上記アクセス制御機構に対しては上記アクセスが不正であることを通知することを特徴としている。

また更に、上記ポリシー設定支援ツールは、上記ポリシー情報に登録された情報とは一部異なるサブジェクトからアクセスが発生した時に、上記アクセス制御機構から通知を受け、上記コンピュータシステムの利用者に対してメッセージを伝え、上記利用者による判断に基づいて所定の処理を実行する手段を備えており、上記利用者による判断とは、上記サブジェクトからのアクセスを許可するか、禁止するかのいずれかであり、上記アクセスを許可する場合には、上記ポリシー設定支援ツールによる所定の処理として上記サブジェクトが正当なものとなるようポリシー情報を変更して、上記アクセス制御機構に対しては上記アクセスが正当であることを通知し、上記アクセスを禁止する場合には、上記ポリシー情報を変更せず、上記アクセス制御機構に対しては上記アクセスが不正であることを通知することを特徴としている。

上記の特徴により、コンピュータシステムの正当な利用を妨げることなく、簡単な操作によりポリシー情報を修正可能となる。

本発明によれば、ポリシーの作成および維持に要する作業負荷を軽減することが可能になる。

These and other benefits are described throughout the present specification. A further understanding of the nature and advantages of the invention may be realized by reference to the remaining portions of the specification and the attached drawings.

## BRIEF DESCRIPTION OF THE DRAWINGS

図 1 は、本実施形態におけるポリシー設定支援ツールの一構成例を示す。

図 2 は、ポリシー設定支援ツールを利用するためのコンピュータシステムの一構成例を示す。

図 3 は、インストール情報と関連付け情報とサンプル情報とアクセスログの一例を示す。

図 4 は、本実施形態において、ポリシー設定画面 4 0 0 の一例を示す。

図 5 は、本実施形態において、ポリシー情報 1 2 0 の一例を示す。

図 6 は、本実施形態において、簡易設定インタフェース 6 0 0 の一例を示す。

図 7 は、サンプル情報 1 0 7 からポリシーを作成する処理のフローチャートを示す。

図 8 は、関連付け情報 1 0 6 からポリシーを作成する処理のフローチャートを示す。

図 9 は、アクセスログ 1 0 8 からポリシーを作成する処理のフローチャートを示す。

図 1 0 は、差分検出部 1 0 4 によるポリシー更新処理のフローチャートを示す。

図 1 1 は、編集用ボックス 4 2 0 に表示するポリシーの変更情報の一例を示す。

図 1 2 は、第二の実施形態におけるポリシー設定支援ツールの一構成例を示す。

図 1 3 は、第二の実施形態におけるポリシーファイル 1 2 2 0 の一例を示す。

図 1 4 は、第二の実勢形態におけるポリシー作成処理のフローチャートを示す。

図 1 5 は、第二の実勢形態におけるポリシー参照・編集画面の一例を示す。

図 1 6 は、アクセス制御部との連携によるポリシー情報変更のフローチャートを示す。

図 1 7 は、変更後のプログラムからアクセスが発生した時に表示するメッセージの一例を示す。

図 1 8 は、未登録のプログラムからアクセスが発生した時に表示するメッセージの一例を示す。

図 1 9 は、新種のファイルに対してアクセスが発生した時に表示するメッセージの一例を示す。



## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

以下、図を用いて第一の実施形態を説明する。

図1は、本実施形態のポリシー設定支援ツールの一構成例である。ポリシー設定支援ツール100は、ユーザインタフェース部101と、ポリシー生成部102、アクセス監視部103、差分検出部104、インストール情報105、関連付け情報106、サンプル情報107、アクセスログ108から構成される。

110はアクセス制御部であり、サブジェクト111からオブジェクト112へのアクセスの可否をポリシー情報120の記述内容に従って判定し、ポリシーに合致したアクセスのみ許可し、ポリシー違反のアクセスであれば上記サブジェクト111にエラーを返すといった処理を行う。

このようなアクセス制御は、一般的なオペレーティングシステム（OS）でも標準で備えているが、それらが参照するポリシー情報の多くは、オブジェクトへアクセス可能なサブジェクトを、ユーザやグループの識別子を用いて指定したものである。

これに対して、本実施形態のポリシー設定支援ツールが扱うポリシー情報とは、ユーザやグループの識別子だけでなく、少なくともアクセスする際に用いるプログラムの情報を組み合わせてアクセス権を指定したものである。

なお、サブジェクト情報113は、本実施例においてはインストールされているプログラムファイル群や、登録されているユーザ・グループに関する情報を指す。

上記ポリシー設定支援ツール100は、上記各種情報105～107や、上記サブジェクト111からオブジェクト112へのアクセスを記録したアクセスログ108を利用しながらポリシー情報120の設定作業を容易にするものである。また、上記サブジェクト情報113を参照しながら、ポリシーの更新作業を容易にするものでもある。

図2は、上記ポリシー設定支援ツール100を利用するために必要なシステムの一例を示したものである。図2において、情報処理装置200は、中央演算処理装置CPU201aと、主記憶202a、外部記憶装置203a、入力装置204、表示部205、LANなどのネットワーク220とのやりとりを制御する通信コントローラ206aが、バスなどの通信線（バスという）207aに接続することで形成されている。

図1にて示したオブジェクト112や、サブジェクト情報113、ポリシー情報120

は、上記外部記憶装置 203 a に格納され、必要に応じて主記憶 202 a の領域に読み出して利用される。

また、上記サブジェクト 111 やアクセス制御部 110 は、主記憶 202 a にロードされ、実行可能プログラムとして上記 CPU 201 a によって処理されるものである。特にアクセス制御部 110 は、オペレーティングシステム (OS) の一部、あるいは OS に組み込み可能なプログラムとして処理される。

同様に、上記ポリシー設定支援ツール 100 も、主記憶 202 a にロードされ、上記 CPU 201 a によって処理されるものである。

また、ポリシー設定支援ツール 100 のうち、ユーザインタフェース部 101 は、上記表示部 205 にユーザインタフェースを表示し、入力装置 204 を介して入力されるデータやコマンドに応じて各種処理を実行する。

また、インストール情報 105 や、関連付け情報 106、サンプル情報 107、アクセスログ 108 については、外部記憶装置 203 a に格納しておき、必要に応じて主記憶 202 a の領域に読み出して利用してもよい。

ここまでは、情報処理装置 200 にて利用されるポリシー情報 120 を、上記ポリシー設定支援ツール 100 により設定および更新するために必要なシステム構成である。

次に、例えば入力装置 204 や表示部 205 をもたないサーバ 210 におけるポリシー設定および更新処理を、上記情報処理装置 200 から行うためのシステム構成について説明する。

サーバ 210 a は、CPU 201 b、主記憶 202 b、外部記憶装置 203 b の他に、通信コントローラ 206 b をバス 207 b に接続することで形成される。通信コントローラ 206 b は、主記憶 202 b にロードされて実行中のプログラムが、ネットワーク 220 を介して他のネットワークノードとデータを交換するために利用する装置である。

上記アクセス制御部 110 が、サーバ 210 a の OS あるいは OS に組み込み可能なプログラムとして主記憶 202 b にロードされて CPU 201 b により処理され、同じく主記憶 202 b にロードされて CPU 201 b により処理されるプログラムをサブジェクト 111 とみなし、当該サブジェクトからオブジェクト 112 へのアクセスを制御することを前提とし、以下説明する。

なお、ポリシー情報 1 2 0 やオブジェクト 1 1 2、サブジェクト情報 1 1 3 は、外部記憶装置 2 0 3 b に格納してもよいし、他のネットワークノードと共有可能な外部記憶装置を別途用意して格納してもよい。

このようなシステム構成において、本実施形態のポリシー設定支援ツール 1 0 0 を利用する場合は、少なくとも入力装置 2 0 4 と表示部 2 0 5 の利用を前提とする上記ユーザインタフェース部 1 0 1 を、情報処理装置 2 0 0 側の主記憶 2 0 2 a にて実行させ、それ以外のポリシー生成部 1 0 2、アクセス監視部 1 0 3、差分検出部 1 0 4 はサーバ 2 1 0 側の主記憶 2 0 2 b にて実行させ、互いにネットワーク 2 2 0 を介してデータ交換を行いながら各種処理を実行する。

また、インストール情報 1 0 5 や、関連付け情報 1 0 6、サンプル情報 1 0 7、アクセスログ 1 0 8 については、外部記憶装置 2 0 3 b に格納してもよいし、他のネットワークノードと共有可能な外部記憶装置を別途用意して格納してもよい。

これにより、遠隔地にある複数のサーバ 2 1 0 b から 2 1 0 x に対しても、同一の情報処理装置からポリシーの設定および更新が可能となる。

図 5 は、上記ポリシー情報 1 2 0 の一例を示したものである。上述のように、本実施形態のポリシー設定支援ツール 1 0 0 が扱うポリシー情報とは、オブジェクトへアクセス可能なサブジェクトを、プログラム名とユーザ・グループの識別子との組み合わせで指定したものである。

図 5 の例で言うと、ユーザ名 "www" の権限で実行しているプログラム " /as/wserv.exe" のみ、オブジェクト名 " /www/pub/\*" で示されるファイル群に対してアクセス "R"（読み出し）を許可するといったものである。図 5 における特徴値とは、プログラムの特徴を表す数値のことであり、例えばプログラムファイルのサイズや、ハッシュ関数を用いて算出した値を利用する。

アクセス発生時に、上記アクセス制御部 1 1 0 が特徴値を確認することで、不当に改ざんされたプログラムによるアクセスからオブジェクトを保護することも可能となる。また、図 5 における時間とは、アクセスを許可する時間帯のことであり、特に指定がない場合は、終日アクセス可能となるよう "00:00-24:00" と設定する。

また、図 5 におけるソフトウェア名称とは、上記プログラムが構成するソフトウェアに

付けられた名称である。これは、利用者がポリシーを編集する際に、ソフトウェア名称を用いてプログラムを指定可能とすることを目的に登録されたものであり、上記アクセス制御部 110 によるアクセス権チェックの際には無視される情報である。

図 3 は、上記インストール情報 105 や、関連付け情報 106、サンプル情報 107、アクセスログ 108 の一例を示したものである。インストール情報 105 とは、上記サブジェクト情報に格納されているプログラムに関する情報を、ソフトウェアの種類毎に分類して管理するためのものである。

その内容は、ソフトウェア名称と、実行ファイル名称、当該実行ファイルのインストール先となるディレクトリ名、更には当該ソフトウェアをアンインストールする際に実行すべきアンインストールプログラムの名称といった情報からなる。

図 3 の例では、“M3 メール 3.0” というソフトウェア名称がインストールされており、その実体となる実行ファイルが“M3MAIL.exe”であり、当該実行ファイルのインストール先が“/m3/”ディレクトリの下であり、アンインストールプログラムの名称が“/m3/uninstall.exe”であることを表している。

このような情報は、一般的なオペレーティングシステム（OS）でも管理している場合が多いことから、本実施形態のポリシー設定支援ツール 100 が独自に管理せずに、OS が管理しているインストール情報を利用することも考えられる。

次に、関連付け情報 106 とは、オブジェクト 112 をアクセスする際に、そのアクセスに利用される頻度の高いプログラムの情報を、オブジェクトの種類毎に管理するためのものである。図 3 の例では、ファイル名の拡張子が“.txt”のオブジェクトへアクセスする際には、利用者からの特別な指示がない限り、実行ファイル名称が“/tools/gpad.exe”のプログラムを利用することを意味している。

このような情報も、一般的な OS が管理している場合が多いことから、本実施形態のポリシー設定支援ツール 100 が独自に管理せずに、OS が管理している関連付け情報を利用することも考えられる。

3 つ目に、サンプル情報 107 とは、ソフトウェアの種類毎に標準的な、あるいは推奨のポリシー情報を記述したものである。図 3 の例では、ソフトウェア名称が“アタッチサーバ 2.0”というプログラムを利用するならば、オブジェクト名が“/www/pub/\*”で表されるファイルに対しては、実行ファイル名称が“/as/wserv.exe”のプログラムが、ユーザ・

グループ名が” www” の権限で実行している場合に限り、アクセスタイプ” R” つまり読み出しのみ許可することを表している。

4つ目に、アクセスログ108とは、上記サブジェクト111からオブジェクト112へのアクセスを、上記アクセス監視部103により監視して、当該アクセス内容を記録したものである。図3に示したアクセスログの一行目の例では、オブジェクト名に示されるファイル” /datafile.db” に対して、サブジェクト情報として示されているプログラム名” /db/hdbr.exe” のプログラムがユーザ名” system” の権限によって、アクセスタイプに示されるアクセス” RW” （読み出しと書き込み）を実行したことを表している。

図4は、ポリシー設定支援ツール100のユーザインタフェース部101が、当該ツールの利用者向けに提供するポリシー設定画面400の一例を示すものである。利用者は、図2の表示部205に表示された上記ポリシー設定画面400を利用することにより、ポリシー情報120の設定や更新、参照といった各種編集作業が可能となる。

ポリシー設定画面400のうち、410aはポリシー情報120に現在登録されているポリシー一覧を表示するボックスである。当該ポリシー表示ボックス410aは、アクセス対象となるオブジェクト名と、アクセス主体となるサブジェクト情報と、許可されたアクセスタイプと、アクセス可能な時間帯を表す情報から構成される。

図4（a）の例では、サブジェクト情報として、ソフトウェアの名称を表示している。これは、図3で示したインストール情報105に格納されているソフトウェア名称と同じものである。これにより、利用者にとってポリシーの概要を把握し易くなるという効果が期待できる。

411aは、ポリシーの表示を切り替えるための切替ボタンであり、利用者が当該切替ボタン411aを押下すると、図4（b）の410bに示すように、サブジェクト情報の表示が、プログラム名とプログラムファイルの特徴値、およびユーザ・グループ名といった、より詳細なものへと切り替わる。反対に、図4（b）の切替ボタン411bを押下すると、図4（a）の410aのような、ソフトウェア名称だけの表示へと切り替わる。

このようなサブジェクト情報の表示切り替えを可能とするためには、上記図3に示したインストール情報105に格納されたソフトウェア名称を、図5に示すようにポリシー情報120に対しても識別子として登録し、各プログラムとソフトウェア名称の対応関係を保持しておけばよい。

または、上記ソフトウェア名称の代わりに、ユニークな識別番号を各ソフトウェアに対して割り当てて、上記インストール情報 1 0 5 と上記ポリシー情報 1 2 0 の両方に登録してもよい。

また、複数のプログラムファイルから構成されるソフトウェアであれば、それらプログラムファイルには全て同一の識別番号あるいは識別子を、上記ポリシー情報 1 2 0 に登録する。多くの場合、それらプログラムファイルの格納先は共通のディレクトリ下であることから、共通のディレクトリ下にあるプログラムファイルに対して同一のソフトウェア識別番号あるいは識別子を割り当てればよい。

上記ユーザインタフェース部 1 0 1 は、上記切替ボタン 4 1 1 が押下される度に、ポリシー情報 1 2 0 を参照しながら上記ポリシー表示ボックス 4 1 0 内のサブジェクト情報の表示内容を切り替えることになる。

4 2 0 は、ポリシーを生成、変更するための編集用ボックスである。4 2 1 は、編集用ボックス 4 2 0 に記述したポリシーを上記ポリシー表示ボックス 4 1 0 に追加して、ポリシー情報 1 2 0 に保存するための追加ボタンである。

上記編集用ボックス 4 2 0 には、オブジェクト名とサブジェクト情報、アクセスタイプ、時間を指定できるが、これら項目を利用者が一つ一つ入力してもよいし、後述するように簡易設定ボタン 4 3 0 を利用して指定することもできる。

また、上記ポリシー表示ボックス 4 1 0 からポリシーを選択すると、上記ユーザインタフェース部 1 0 1 が、当該ポリシーを上記編集用ボックス 4 2 0 に表示するので、既に登録済みのポリシーを一部変更する際には、上記ポリシー表示ボックス 4 1 0 に表示されたポリシーから変更したいものを選択して上記編集用ボックス 4 2 0 に表示し、必要な修正を加えてから上記追加ボタン 4 2 1 を押下すればよい。

上記ポリシー設定画面 4 0 0 には、上記簡易設定ボタン 4 3 0 の他、サンプル登録ボタン 4 3 1、更新ボタン 4 3 2、削除ボタン 4 3 3、終了ボタン 4 3 4 がある。以下、これらボタンの意味について説明する。

簡易設定ボタン 4 3 0 は、上記サンプル情報 1 0 7 や、関連付け情報 1 0 6、アクセスログ 1 0 8 等を利用して、ポリシー原案を自動生成する際に押下するボタンである。当該処理については後述する。

サンプル登録ボタン431は、上記編集用ボックス420の表示内容を上記サンプル情報107に登録し、以後サンプルポリシーとして再利用可能なものとする際に押下するボタンである。

更新ボタン432は、上記ポリシー情報120に登録されているポリシーを、最新のオブジェクトやサブジェクト情報113に合わせて更新する際に押下するボタンである。この処理についても後述する。

登録済みのポリシーを一部削除したい場合には、上記ポリシー表示ボックス410に表示されたポリシーから削除したいものを選択して、削除ボタン433を押下する。また、ポリシー編集作業を終了する場合には、終了ボタン434を押下する。

図6は、上記簡易設定ボタン430を押下したときに、図2の表示部205に出現する簡易設定インタフェースの一例を示したものである。利用者は、簡易設定インタフェース600を通じて、上記サンプル情報107を利用したポリシー原案作成や、上記関連付け情報106を利用したポリシー原案作成、更には上記アクセスログ108を利用したポリシー原案作成を実行することができる。

図6の601は、インストールされているソフトウェア一覧表示ボックスであり、上記ユーザインタフェース部101が、上記インストール情報105およびサンプル情報107を参照して、現在インストールされていて且つサンプルポリシーが用意されているソフトウェアのみを表示する。

利用者が、これらソフトウェアのサンプルポリシーを利用してポリシーの原案を作成する場合には、各ソフトウェアに対応したチェックボックス603aにチェックを付けて、原案作成ボタン608を押下すればよい。

図6の602は、特定のソフトウェアとの関連付けがされているファイル拡張子一覧表示ボックスであり、上記ユーザインタフェース部101が上記関連付け情報106を参照して表示する。当該関連付け情報を利用してポリシーの原案を作成する場合には、各拡張子に対応したチェックボックス603bにチェックを付けて、原案作成ボタン608を押下すればよい。

図6の605は、監視したいプログラムを指定するための入力ボックスであり、ここにプログラムファイル名を入力して開始ボタン606を押下すると、上記アクセス監視部によるアクセス監視と上記アクセスログ108への記録を開始する。終了ボタンを押下する

と、上記アクセス監視とアクセスログ記録を終了する。

その後で、上記原案作成ボタン608を押下すると、アクセスログ108を利用してポリシー原案を作成することができる。なお、上記プログラムの指定は、プログラムファイル名の代わりに、ソフトウェアの名称で指定できるものでもよい。

上記のように作成されたポリシー原案は、上記ユーザインタフェース部101の処理により、図4の編集用ボックス420に表示される。当該ポリシー原案をベースに、利用者が一部修正を加えるなど、編集作業を行ってから上記追加ボタン421を押下すると、当該編集されたポリシーを上記ポリシー表示ボックス410に追加すると共に、ポリシー情報120にも保存する。

図6の609は、キャンセルボタンであり、上記簡易設定インタフェース600の処理を終了して、図4のポリシー設定画面400へ戻る際に押下する。

図7は、サンプル情報107からポリシー原案を生成する処理手順の一例を示したものである。ステップ701は、上記ユーザインタフェース部101へのコマンド入力であり、これは図6のソフトウェア一覧表示ボックス601からソフトウェアを選択して、上記原案作成ボタン608を押下することに相当する。

ステップ702では、上記ポリシー生成部102により、上記選択されたソフトウェアに対応するサンプル情報を取得する。ステップ703では、上記差分検出部103により、上記サブジェクト情報113やオブジェクト112を参照して、上記サンプル情報との差分データを作成する。

これは、ソフトウェアのインストール先や、ディレクトリ構成が標準と異なる場合、上記サンプル情報がそのまま利用できないことがあるためである。ステップ704では、上記ポリシー生成部102により、上記サンプル情報と差分データを基に、対象となる情報処理装置やサーバに相応しいポリシーの原案を生成する。

このとき、アクセス許可されるプログラムの特徴値算出も併せて行う。また、アクセス許可する時間帯については、特に指定がない限り、終日(00:00-24:00)に設定しておく。ステップ705では、上記ユーザインタフェース部101により、上記ポリシーの原案を、上記図4の編集用ボックス420に表示する。

ステップ706では、表示されたポリシー原案に対して、利用者自身により必要な修正



を加える。この修正とは、例えばアクセス許可する時間帯の指定や、ユーザ・グループの指定変更等である。ステップ707では、上記修正後のポリシーを、上記ポリシー情報120へ保存する。このとき、サブジェクト情報として、プログラム名、特徴値、ユーザ・グループ名の他、ソフトウェア名称も付加して保存する。

次に図8を用いて、関連付け情報106を利用したポリシー生成の処理手順の一例を説明する。ステップ801は、上記ユーザインタフェース部101へのコマンド入力であり、これは図6のファイル拡張子一覧表示ボックス602から拡張子を選択して、上記原案作成ボタン608を押下することに相当する。

ステップ802では、上記関連付け情報106を参照して、上記利用者が選択した拡張子に関連付けられたプログラムの実行ファイル名称を取得する。ステップ803では、上記ポリシー生成部102により、上記取得した情報を基にポリシーの原案を生成する。

このとき生成されるポリシーの原案は、オブジェクト名と、プログラム名と、プログラムの特徴値と、時間帯のみ指定されており、ユーザ・グループ名やアクセスタイプは指定していない。ただし、図2に示した上記情報処理装置200やサーバ210が利用しているOS自身が、上記アクセス制御部110とは異なる独自のアクセス制御機構を備えている場合はその通りでない。

つまり、当該OS独自のアクセス制御機構があれば、各オブジェクトへのアクセス条件として、ユーザ・グループの情報や、アクセスタイプが設定されているはずである。そこで、例えば上記ポリシー生成部102がこれらユーザ・グループの識別子やアクセスタイプを取得して、上記ポリシーの原案に取り込むものであってもよい。

また、同じ拡張子をもつファイルでも、これらユーザ・グループやアクセスタイプが異なるものは、オブジェクト名を区別してそれぞれ個別のポリシーとなるよう原案を作成する。

このようにして生成したポリシー原案は、ステップ804にて上記ユーザインタフェース部101が、上記図4の編集用ボックス420に表示する。ステップ805では、表示されたポリシー原案に対して、利用者自身により必要な修正を加える。

この修正とは、例えばアクセス許可する時間帯の指定や、ユーザ・グループの指定変更等である。ステップ806では、上記修正後のポリシーを、上記ポリシー情報120へ保存する。

このとき、サブジェクト情報として、プログラム名、特徴値、ユーザ・グループ名の他、ソフトウェア名称も付加して保存する。当該ソフトウェア名称は、上記インストール情報 105より取得する。

次に図9を用いて、上記アクセスログ108を利用したポリシー生成処理手順の一例を説明する。ステップ901は、上記ユーザインタフェース部101へのコマンド入力であり、これは図6の入力ボックス605にプログラムを指定して、上記開始ボタン606を押下することに相当する。

ステップ902では、上記アクセス監視部103により、上記指定されたプログラムから発行されるファイルアクセスを監視して、その内容を上記アクセスログ108に記録する。この処理は、上記図6の終了ボタン607を押下するまで継続する。

ステップ903では、上記ポリシー生成部102により、上記アクセスログ108からポリシー原案を生成する。このとき、上記アクセスログ108に記録されたアクセスは、正当なアクセスとして許可されるようにポリシー原案を作成する。

また、サブジェクトとなるプログラムの特徴値も算出し、上記ポリシー原案に取り入れる。時間帯指定については、特に指定がない限り”00:00-24:00”（終日）とする。

このようにして生成したポリシー原案は、ステップ904にて上記ユーザインタフェース部101が、上記図4の編集用ボックス420に表示する。ステップ905では、表示されたポリシー原案に対して、利用者自身により必要な修正を加える。

この修正とは、例えばアクセス許可する時間帯の指定や、ユーザ・グループの指定変更等である。ステップ906では、上記修正後のポリシーを、上記ポリシー情報120へ保存する。

このとき、サブジェクト情報として、プログラム名、特徴値、ユーザ・グループ名の他、ソフトウェア名称も付加して保存する。当該ソフトウェア名称は、上記インストール情報 105より取得する。

以上の図7から図9の処理を、利用者が必要に応じて繰り返したり、組み合わせたりしながらポリシーを作成することになる。

次に、図 10 を用いて上記差分検出部 104 の処理手順について説明する。これは、上記オブジェクト 112 やサブジェクト情報 113 に変更が生じた場合にも、登録済みのポリシー情報 120 への反映を容易にするための処理である。

ステップ 1001 は、例えば上記ユーザインタフェース部 101 へのコマンド入力であり、これは上記図 4 の更新ボタン 432 を押下することに相当する。あるいは、図 2 の上記情報処理装置 200 やサーバ 210 に搭載された OS が備えるスケジューラ機能等により、差分検出部 104 の処理を定期的に行わせるものであってもよい。

そして差分が検出された場合には、ポリシーの記述を見直す必要があることを、上記ユーザインタフェース部 101 を通じて利用者に通知することで、無効なポリシーの記述を放置することなく、常に適切なポリシーに基づくアクセス制御が可能となる。

ステップ 1002 では、差分検出部 104 が上記ポリシー情報 120 を参照し、当該ポリシー情報 120 に登録されているオブジェクト名とサブジェクト情報を取得する。ステップ 1003 では、オブジェクトとサブジェクトに関する最新情報を、上記オブジェクト 112 とサブジェクト情報 113 とから取得し、上記ポリシー情報 120 の内容と照合する。

ステップ 1004 では、上記照合処理の結果、更新の必要があると思われるポリシーについてはその内容を上記ユーザインタフェース部 101 に渡し、図 11 に示すように、上記編集用ボックス 420 に表示する。このとき、変更のあった部分が他よりも目立つよう強調表示する。

利用者は、当該変更内容を目視で確認し（ステップ 1005）、更新しても問題ないと判断するならば、必要な修正を加えた上で、図 11 の更新ボタン 422 を押下することで、正式に上記ポリシー情報 120 の内容を更新できる（ステップ 1006）。仮に、プログラムのアップデートをした覚えがないのに、プログラムの特徴値に変更があった場合は、プログラムファイルの不当な改ざんが発生した可能性もあると考えられ、この場合は、利用者はポリシーの更新をせずに上記プログラムファイル改ざんの原因を確認すればよい。

以上述べたように、本実施形態によれば、ソフトウェアの仕様を詳しく知らなくても、ソフトウェアの種類毎に用意したサンプルポリシーや、関連づけ情報、ソフトウェアのアクセスログを利用することで、適切なポリシーを短時間に作成することができる。

また、オブジェクトやサブジェクトの情報に変更があった場合でも、変更すべきポリシ

一の部分が利用者にとって容易に判るよう表示でき、且つ簡易な操作で更新可能であることから、常に適切なポリシー情報に基づくアクセス制御が可能となる。

次に、第二の実施形態を説明する。

図12は、第二の実施形態となるポリシー設定支援ツールの一構成例である。ポリシー設定支援ツール1200は、ユーザインタフェース部1201と、ポリシー生成部1202、差分検出部1204から構成され、インストール情報105や、関連付け情報106、オブジェクト共有情報109、サブジェクト情報113を参照しながらポリシーを生成し、ポリシーファイル1220に登録する役割をもつ。なお、サブジェクト情報113は、本実施例においてはインストールされているプログラムファイル群を指す。

110はアクセス制御部であり、サブジェクト111からオブジェクト112へのアクセスの可否をポリシーファイル1220の記述内容に従って判定し、ポリシーに合致したアクセスのみ許可し、ポリシー違反のアクセスであれば上記ポリシー設定支援ツール1200を通じてユーザ1210に通知し、その応答を受けて上記サブジェクト111にエラーを返す、あるいはアクセスを許可するといった処理を行う。

1240は認証処理部であり、ユーザ情報1230に登録されている情報を参照しながらユーザ1210の識別と認証の処理を行う。ユーザ1210は、上記オブジェクト112を利用するのに先立って、上記認証処理部1240による識別認証を受ける必要がある。このとき、ユーザ1210は例えば自己のユーザIDとパスワードを入力することになり、ユーザ情報1230と一致すれば、以後サブジェクト111を実行してオブジェクト112へのアクセスを発行できるようになる。なお、上記サブジェクト111は、例えば実行中のプログラムであり、且つ当該プログラムを実行したユーザのIDを継承しており、上記アクセス制御部110が許可する範囲でオブジェクト112へアクセス可能となる。

このような認証処理部とアクセス制御部は、一般的なオペレーティングシステム（OS）でも標準で備えているが、それらが参照するポリシー情報の多くは、オブジェクトへアクセス可能なサブジェクトを、ユーザやグループの識別子を用いて指定したものである。

これに対して、第二の実施形態のポリシー設定支援ツールが扱うポリシー情報とは、オブジェクトの種類毎にアクセス可能なプログラムを指定したものである。

つまり第二の実施形態におけるアクセス制御部110は、例えば一般的なOSが備えるアクセス制御機能と、上記ポリシー設定支援ツールが扱うポリシー情報を用いたアクセス

制御機能とを併せ持つものと言える。このうち、一般的なOSが備えるアクセス制御機能では、図13の1300に示すようなポリシー情報を参照する。これは、ファイル名と、その所有者名と、アクセス権から構成され、全てのファイルやディレクトリに対して必ず何らかのアクセス権が設定されている。アクセス権は更に3種類のユーザに対するアクセス権を指定でき、左から順に、所有者のアクセス権、所有者と同じグループに属するユーザのアクセス権、所有者とは異なるグループに属するユーザのアクセス権、となっている。図中のRWDXはアクセスのタイプを表し、それぞれ読み出し(R)、書き込み(W)、削除(D)、実行またはチェンジディレクトリ(X)を意味する。通常、このようなポリシー情報1300は、OSが標準で備えるツール等を用いて設定できる。

一方、図13の1310は、ポリシー設定支援ツール1200によって設定するポリシー情報であり、ファイルの種類と、プログラム名と、プログラムの特徴値から構成される。上記ポリシー情報1300に示すように、従来のアクセス権はファイルやディレクトリ毎に指定するものであったが、ポリシー情報1310ではアクセスに用いるプログラムをファイルの種類毎に設定することが特徴である。これは、一般的にファイルの種類が異なれば利用するプログラムも異なるという点に着目し、プログラムを指定する場合には個々のファイルやディレクトリ単位でなく、ファイルの種類毎に指定することが有効であるとの考えに基づく。ファイルの種類はファイル名の拡張子によって区別でき、例えばHTMLファイルであれば“\*.html”のように記述すれば、拡張子htmlをもつ全てのファイルを指定したことになる。また、全種類のファイルを指定する場合には、“\*.\*”と記述すればよい。なお、上記特徴値とはプログラムの特徴を表す数値のことであり、例えばプログラムファイルのサイズや、ハッシュ関数を用いて算出した値を利用する。

ここで、ポリシー情報1300を例にとると、ファイル“/users/satou/memo.txt”は、ユーザ satou によってRWDが可能となるが、ポリシー情報1310によれば、拡張子が“txt”のファイルに対しては、いかなるユーザであっても“/tools/gpad.exe”のプログラム、あるいは全てのファイル(\*.\*)にアクセス可能なプログラムを利用する必要がある。また別の言い方をすれば、全てのファイルにアクセス可能なプログラムとしてポリシー情報1310に登録されたプログラムを用いてファイル“/users/satou/memo.txt”にアクセスしても、ポリシー情報1300の方で上記ファイルにアクセス権を与えられたユーザでなければ、上記アクセス制御部110によりアクセスは禁止される。これにより、ポリシー情報1300のみを利用していた従来のアクセス制御と比べ、ポリシー情報1310を併せて利用することで不正なプログラムによるアクセスを防止でき、厳重なオブジェクト管理を実現できる。

このようなポリシー情報1310を簡易な操作で設定可能とするポリシー設定支援ツ-

ル１２００を利用するために必要なシステムは、上記第一の実施形態と同様に、図２の情報処理装置２００が一例として挙げられる。

図２において、情報処理装置２００は、中央演算処理装置ＣＰＵ２０１ａと、主記憶２０２ａ、外部記憶装置２０３ａ、入力装置２０４、表示部２０５、通信コントローラ２０６ａが、バスなどの通信線（バスという）２０７ａに接続することで形成されている。

図１２にて示したオブジェクト１１２や、サブジェクト情報１１３、インストール情報１０５、関連付け情報１０６、オブジェクト共有情報１０９、ポリシーファイル１２２０、ユーザ情報１２３０は、上記外部記憶装置２０３ａに格納され、必要に応じて主記憶２０２ａの領域に読み出して利用される。このうち、サブジェクト情報１１３と、インストール情報１０５、関連付け情報１０６の内容は、第一の実施形態の説明に用いたものと同じである。

また、上記サブジェクト１１１やアクセス制御部１１０、認証処理部１２４０は、主記憶２０２ａにロードされ、実行可能プログラムとして上記ＣＰＵ２０１ａによって処理されるものである。特にアクセス制御部１１０と認証処理部１２４０はＯＳの一部、あるいはＯＳに組み込み可能なプログラムとして処理される。

同様に、上記ポリシー設定支援ツール１２００も、主記憶２０２ａにロードされ、上記ＣＰＵ２０１ａによって処理されるものである。

また、ポリシー設定支援ツール１２００のうち、ユーザインタフェース部１２０１は、上記表示部２０５にユーザインタフェースを表示し、入力装置２０４を介して入力されるデータやコマンドに応じて各種処理を実行する。

図１４は、上記ポリシー設定支援ツール１２００によるポリシー情報の作成処理フローを示したものである。当該作成処理は、例えばポリシー設定支援ツール１２００を上記情報処理装置２００へインストールした時や、ユーザ１２１０が上記ツール１２００を起動した時に自動的に開始するものであってもよい。または、上記ツール１２００が定期的に行う実行するものでもよい。更には、後述する図１５に示すポリシー参照・編集画面１５００にある更新ボタン１５０８をユーザ１２１０が押下した時でもよい。

ステップ１４０１では、差分検出部１２０４が、関連付け情報１０６に登録されているファイルの種類と、上記ポリシー情報１３１０に登録されているファイルの種類を比較して、その差分を検出する。このうち、ポリシー情報１３１０に登録されていて、且つ関連

付け情報 106 に登録されていないファイルの種類があれば、ポリシー情報 1310 から当該ファイルの種類に関する記述を削除する。一方、ポリシー情報 1310 に未登録のファイルの種類があれば、ステップ 1402 で各ファイルの種類毎に関連付けられたプログラム（実行ファイル）の名称を、関連付け情報 106 から取得する。このとき、図 19 に示すようなメッセージボックス 1900 を表示部 205 に表示してユーザ 1210 に確認してもよい。ここで、ユーザがボタン 1901 「はい」を押下すればステップ 1403 の処理へ移り、ボタン 1903 「いいえ」を押下すれば差分検出処理（ステップ 1401）に戻る。あるいは、関連付けられたプログラムであれば、逐一ユーザに確認することなくステップ 1403 の処理へ移るといった実施形態も考えられる。

ステップ 1403 では、サブジェクト情報 113 から上記実行ファイルの特徴値を算出してポリシー情報 1310 を生成する。また、既にポリシー情報 1310 に登録されている実行ファイルのうち、特徴値が変更されているものがあれば、上記差分検出部 1204 からユーザインタフェース部 1201 へその旨通知し、ステップ 1404 にて図 17 に示すようなメッセージボックス 1700 を表示部 205 に表示してユーザ 1210 に確認する。上記メッセージボックス 1700 において、ユーザがボタン 1701 「はい」を押下すれば、変更後のプログラムは正当なプログラムであるとして上記ポリシー情報 1310 を更新する。また、ボタン 1702 「いいえ」を押下すれば、上記ポリシー情報 1310 は更新しない。

ステップ 1405 では、上記ユーザインタフェース部 1201 が、上記処理により生成したポリシー情報 1310 を、図 1-5-0 のポリシー参照・編集画面 1500 の形式で表示部 205 に表示する。上記関連付け情報 106 から生成したポリシーは、図 1-5-0 中の「ファイルの種類とプログラムの対応一覧」1501 に含まれている。

当該一覧 1501 には、OS を構成する各種プログラム（システムプログラムと呼ぶ）と関連付けられたファイルの種類と、上記 OS 上で動作するアプリケーションプログラムと関連付けられたファイルの種類とが混在することになる。両者を区別して表示するために、ポリシー設定支援ツール 1200 は、先ずアプリケーションプログラムの名称を上記インストール情報 105 から取得し、次にそれらアプリケーションプログラムと関連付けられたファイルの種類を上記関連付け情報 106 より取得する。そして、それ以外のもの、つまり上記システムプログラムと関連付けられたファイルの種類とは、色分けして上記一覧 1501 に表示する。

このように表示された上記一覧 1-5-0-1 の設定内容を上記ポリシーファイル 1-2-20 に格納するためには、保存ボタン 1-5-0-9 を押下する。このとき、ポリシー情報 1-3-10 が

ら除外したい関連付けがあれば、そのチェックボックス1505のマーク（レ印）を外してから保存ボタン1509を押下すればよい。ただし、除外されたファイルの種類に対しては、どのプログラムを用いてアクセスしてもよいことになる。

ここで、上記関連付け情報106から作成したポリシー情報1310のもとでは、別のプログラムとの間でオブジェクトを共有する機能をもつプログラムが正常に動作しなくなる場合がある。たとえば、表計算の機能がないワープロソフトが、その文書中に、表計算ソフトで作ったグラフを貼り込めるうえ、グラフに変更を加えたい場合は、ワープロ文書中のグラフをダブルクリックすることにより表計算ソフトが自動的に起動する、といった機能を持つ場合である。表計算ソフトで作成したグラフは、もともと表計算ソフトと関連付けられた種類のファイルに格納されているため、上記ワープロソフトから上記グラフを貼り込むときに、関連付けられていないファイルへのアクセスが発生する。当該アクセスは、上記関連付け情報106から作成したポリシー情報1310により、不正なアクセスとして扱われることになる。

これらアクセスを許可するのであれば、上記ポリシー設定支援ツール1200が、（1）オブジェクトの共有機能をもつプログラムの名称（2）上記プログラムから貼り込み可能なオブジェクトの種類（3）上記オブジェクトの格納元となるファイルの種類順に情報を取得し、（1）のプログラムから（3）のファイルの種類へのアクセスを許可するポリシーを生成して上記ポリシー情報1310に追加すればよい。このとき、上記プログラムの特徴値についても、上記サブジェクト情報113から算出して登録する。上記（1）から（3）までの情報をあわせて、ここではオブジェクト共有情報109とする。当該オブジェクト共有情報109は、OSがコンピュータに関するあらゆる設定情報を集中管理するためのデータベースに含まれており、そこには上記関連付け情報106やインストール情報105も格納されている。

図15で言えば、プログラム間でオブジェクトの共有を許可するためのチェックボックス1502にマーク（レ印）をつけて保存ボタン1509を押下すると、上記ポリシー設定支援ツール1200が上記データベースの情報をもとに、自動的にポリシー情報1310を作成して保存する。更に、詳細設定ボタン1503を押下すると上記オブジェクト共有情報を詳細設定画面1520に表示し、プログラム毎に貼り込み可能なオブジェクトの種類、つまりアクセス可能なファイルの種類をきめ細かく設定できるようにしても良い。

当該詳細設定画面1520では、オブジェクトの共有機能をもつプログラムをプルダウンメニュー1521から選択し、当該プログラムから貼り込み可能なオブジェクトを、オブジェクトとファイルの種類の一覧表示ボックス1522にて選択指定（マーク付与）す



ればよい。実際には、初期設定時に上記チェックボックス1502にマークを付ければ、上記ボックス1522では貼り込み可能なオブジェクト全てにチェックマークが付いた状態となるようにし、そこから不要なものがあればマークを消していくことにする。例えば、オブジェクト「3D図面」が標準で格納されているファイル「\*.fig」に対して、プログラム「/ap/wordproc.exe」からアクセスすることが業務上不要であれば、詳細設定画面1520にて、上記オブジェクト「3D図面」のマークを消せばよい。以上のやり方で設定したポリシーは、保存ボタン1509を押下することでポリシー情報1310に反映される。

次に、ポリシー参照・編集画面1500におけるプログラム指定ボックス1504は、例えば業務遂行上、各種ファイルへアクセスする際に用いるプログラムを指定するためのボックスである。これらも、関連付け情報106から作成したポリシーだけでは正常に動作しないと思われるプログラムであり、例えば各ファイルのコピーや移動、削除といったファイル操作のプログラムや、コンピュータウィルスを検出して駆除するためのウィルス対策ソフト、障害時に重要なファイルを復旧するためのバックアップツール、ファイルの圧縮・解凍ツールなどがある。その他、電子メールやWWWにより各種ファイルを送受信するケースも考えられる。プログラム指定ボックス1504では、ユーザにとって分かり易くなるように、これらプログラムを用途別に指定可能とする。

ポリシー情報1310の初期設定時は、いずれのプログラムも指定されていない状態となるが、OSが標準で備えているプログラムがある場合は、ポリシー設定支援ツール1200が上記インストール情報105からそれらプログラムのソフトウェア名称を取得して、上記プログラム指定ボックス1504に表示してもよい。これにより、ユーザ1210によるプログラム選択作業を軽減できる。OSが標準で備えるプログラムとは異なるものを指定する場合には、ユーザ1210または上記情報処理装置200の管理者が参照ボタン1506を押下すると、上記インストール情報105からソフトウェア名称の一覧が表示され、その一覧から任意のプログラムを選択指定できる。インストール情報105に登録されていないソフトウェアであれば、プログラムファイル名を直接指定してもよい。また、電子メールやブラウザによるファイル送受信は、情報セキュリティを考えれば控えたほうが望ましいので、別の実施形態として、これらのプログラムは上記プログラム指定ボックス1504から選択指定できなくしてもよい。

上記のようにプログラムを選択してから保存ボタン1509を押下すると、上記ポリシー生成部1202はサブジェクト情報113から該当するプログラムファイルを検索してその特徴値を算出するとともに、そのプログラムが全種類のファイル(\*.\*)に対してアクセス可能となるようポリシー情報1310を作成し、上記ポリシーファイル1220

に保存する。その他の方法として、上記プログラムによってアクセス可能な対象は全種類のファイルでなく、例えばアプリケーションプログラムと関連付けられた種類のファイルに対してアクセス可能となるようポリシー情報 1310 を作成するものであってもよい。もしくは、アクセス可能な対象を更に細かく指定するために、ファイルの種類の一覧表示から選択指定させるものであってもよい。用途別に指定されたプログラムに対しては、その用途についても併せてポリシー情報 1310 に登録しておくことで、以後のポリシー情報設定時に、現在の設定内容をプログラム指定ボックス 1504 に表示することが可能となる。

また、ファイルのネットワーク共有を許可するためのチェックボックス 1507 を有効にして保存ボタン 1509 を押下すると、各種ファイルがネットワークで共有可能となるようポリシー情報 1310 を作成して保存する。このときアクセス権を与えるべきプログラムは、OS が標準で備えているファイル共有用のサーバプログラムであるが、通常のアプリケーションプログラムとは異なり上記インストール情報 105 には登録されていない場合があるため、本実施例のように上記プログラム指定ボックス 1504 とは区別して扱ってもよい。

更新ボタン 1508 は、上記ポリシー作成処理フロー（ステップ 1401 から 1405）の処理を繰り返してポリシー情報 1310 を更新するときに押下するボタンである。また、閉じるボタン 1510 を押下すれば、ユーザインタフェース部 1201 の処理を終了してポリシー参照・編集画面 1500 を表示部 205 から消す。

次に、上記アクセス制御部 110 とポリシー設定支援ツール 1200 の連携によりポリシー情報 1310 を適宜変更していく方法を、図 16 を用いて説明する。

ステップ 1601 では、上記サブジェクト 111 からオブジェクト 112 へのアクセスをアクセス制御部 110 により検知し、ステップ 1602 にて上記アクセスをポリシーファイル 1220 の記述内容と照合する。このとき、一般的な OS が備えるアクセス制御ではポリシー情報 1300 との照合によりアクセス権を判定するが、本実施の形態においてはポリシー情報 1310 との照合も併せて実施し、いずれのポリシーにも合致したアクセスであれば「適合」とみなしてステップ 1609 にて当該アクセスを許可する。

上記アクセスがポリシー情報 1300 と合致しない場合、上記アクセス制御部 110 はアクセス要求元となるサブジェクト（プログラム）へ直ちにエラーを返して上記アクセスを禁止するが、ポリシー情報 1310 と合致しない場合には、ポリシー設定支援ツール 1200 の処理に移り、ステップ 1603 以降の処理を実行する。ステップ 1603 では、

アクセス制御部110からの通知内容に基づいてメッセージを表示部205に表示する。このとき表示するメッセージには3種類あり、サブジェクト（プログラム）の特徴値が一致しない場合には図17を、サブジェクト（プログラム）の名称が一致しない場合には図18を、オブジェクト情報（ファイルの種類）がポリシーに登録されていない場合には図19をそれぞれ表示する。

図17のメッセージボックス1700では、アクセス要求元となるプログラムの特徴値がポリシー情報1310の記述と一致しない場合に、プログラムが変更されている可能性があることをユーザ1210に伝えるものである。ステップ1604では、ユーザ1210は「はい」ボタン1701か、「いいえ」ボタン1702のいずれか一つを選んで押下することになる。「はい」ボタン1701を押下すると、ステップ1605にてポリシー設定支援ツール1200はポリシー情報1310を変更（特徴値を変更）し、上記アクセス制御部110に上記アクセスが「適合」であることを通知する。「いいえ」ボタン1702を押下すると、正当なプログラムではないとみなして、ステップ1607にてポリシー情報1310は変更せず、上記アクセス制御部110に上記アクセスが「違反」であることを通知する。その他の実施形態として、ユーザ1210による判断だけでなく、例えば図2に示したネットワーク220を介して、上記変更されたプログラムが正当なものかどうかを、当該プログラムを製造または販売しているサイトへ問い合わせるためのボタンを、上記メッセージボックス1700に追加することも考えられる。この場合、各プログラム毎にその製造または販売元となるサイトの情報（アドレス）を、上記インストール情報105やポリシー情報1310にて保持しておき、ユーザが上記問い合わせ用のボタンを押下したときに該当するサイトへ自動的に問い合わせるなどの処理が必要となる。

図18のメッセージボックス1800は、ある種類（例えば拡張子がdoc）のファイルに対してアクセス権をもたないプログラムからアクセス要求があった場合に、不正なプログラム、あるいは未登録のプログラムからのアクセスであることをユーザ1210に伝えるものである。ステップ1604では、ユーザ1210は「はい」ボタン1801か、「今回のみ」ボタン1802か、「いいえ」ボタン1803のいずれか一つを選んで押下することになる。「はい」ボタン1801を押下すると、以後上記プログラムから上記種類（拡張子がdoc）のファイルへのアクセスを許可するよう、ステップ1605にてポリシー情報1310を変更し、上記アクセス制御部110に上記アクセスが「適合」であることを通知する。「今回のみ」ボタン1802を押下すると、ステップ1606にてポリシー情報1310は変更せずに上記アクセスが「適合」であることを通知する。これにより、今回のアクセスは許可されるが、次回同じアクセスが発生した場合は再度メッセージボックス1800が表示されることになる。また、「いいえ」ボタン1803を押下すると、不正なアクセスとみなして、ステップ1607ではポリシー情報1310は変更せず、上記アク

セスが「違反」であることを通知する。

図19のメッセージボックス1900は、ポリシー情報1310に登録されていない種類のファイルに対してアクセス要求があった場合に、ポリシー設定支援ツール1200が上記関連付け情報106から上記種類のファイルに関する関連付け情報を取得し、ユーザ1210に伝えるものである。ただし上記メッセージボックス1900は、上記種類のファイルと関連付けられたプログラムからのアクセス要求であった場合に表示するものであり、関連付けられたプログラム以外からのアクセス要求であった場合の処理は、上記メッセージボックス1800で説明した通りである。メッセージボックス1900では、ユーザ1210は「はい」ボタン1901か、「いいえ」ボタン1903のいずれか一つを選んで押下することになる。「はい」ボタン1901を押下すると、ステップ1605にてポリシー設定支援ツール1200は上記関連付けられたプログラムからのアクセスが以後許可されるようにポリシー情報1310を変更し、上記アクセス制御部110に上記アクセスが「適合」であることを通知する。「いいえ」ボタン1903を押下すると、上記関連付け情報は妥当でないとみなして、ステップ1607にてポリシー情報1310は変更せず、上記アクセス制御部110に上記アクセスが「違反」であることを通知する。

以上述べた第二の実施の形態で、情報セキュリティの観点から見た有効な使い方を述べる。例えば電子メールやブラウザなどの通信機能をもつプログラムは、不正なプログラムの持ち込みや機密情報流出といったセキュリティホールとなる恐れがあるので、全種類のファイルにアクセス可能なプログラムとして指定しないことが望ましい。ポリシー設定支援ツール1200が関連付け情報106から生成したポリシー情報1310であれば、電子メールやブラウザから利用できるファイルの種類は限定される。もし、業務の中で電子メールやブラウザを用いて文書ファイルを送受信する必要があった場合には、当該文書ファイルへのアクセス時に上記メッセージボックス1800が表示されるので、そこで「今回のみ」ボタン1802を選べばよい。これにより業務には支障なく、且つ不正なプログラムによるファイル送受信を防止することが可能となる。

上記ポリシーファイル1220、特にポリシー情報1310が不当に書き換えられないようにするためには、例えばポリシーファイル1220へアクセス可能なプログラムを、ポリシー設定支援ツール1200に限定するよう、予めポリシー情報1310に記述しておくことが有効である。

また、企業などの組織で運用する場合には、ポリシー情報1310は組織で決定するものであり、ユーザ1210によってポリシー情報1310を任意に変更されるのは好ましくないケースもある。つまり、上記ポリシー設定支援ツール1200は組織で決めたポリ

シーを設定する際に管理者が利用するものであり、それ以外の状況で管理者以外の人物が利用するものではない。この場合は、上記ポリシーファイル1220へアクセス可能なプログラムの限定に加えて、ポリシーファイル1220には例えばOSの管理者だけがアクセス可能となるよう、予めポリシー情報1300に記述しておくことが有効である。ただし、OS管理者の認証情報（例えばパスワード）が一般ユーザに悪用されないよう、厳重に管理しておく必要はある。

更に、管理者以外のユーザ1210に対しては、上記アクセス制御部110によるメッセージボックス1700～1900の表示処理は提供せず、ポリシー情報1310に違反するアクセスが発生したときには無条件にエラーを返すものとする。これは、図16のステップ1602で違反と判定した場合に、ステップ1610の処理へジャンプすることに相当する。このような管理者向けと一般ユーザ向けの処理の切り替えは、環境設定情報として上記ポリシーファイル1220の一部に格納しておき、上記アクセス制御部110がその環境設定情報を参照し、管理者向けであれば図16のステップ1603から1608の処理を追加し、その他一般ユーザ向けであればポリシー情報1310に違反するアクセスは全てエラーを返すようにすればよい。

また、多数の情報処理装置にて共通のポリシー情報を利用するならば、上記ポリシー設定支援ツールにより作成したポリシー情報を、各情報処理装置に配布して利用することで運用管理上の負荷を軽減することも可能である。特に、第二の実施形態にて示したポリシー情報1310は、ファイルのパス名でなく種類毎にポリシーを記述したものであるため、ファイルの移動やコピー、削除等が発生してもファイルの種類が変わらない限り同一のポリシー情報1310にて保護可能となる。したがって、各情報処理装置で共通のポリシー情報1310を利用すれば、同じセキュリティ効果が期待できる。

各情報処理装置で共通のポリシー情報1310を作成する方法としては、上記第二の実施形態で述べたように、設定対象となる情報処理装置にインストールされたポリシー設定支援ツール1200を用いてもよいが、更に運用管理上の負荷を軽減するために、ネットワーク220を介して接続されているリモートのサーバまたは情報処理装置から設定する方法も考えられる。この場合、例えば設定対象となる情報処理装置にて図示していない代理プログラムを実行し、ネットワーク220を介してリモートのサーバまたは情報処理装置にて実行するポリシー設定支援ツール1200と通信可能な状態をつくり、上記代理プログラムからは設定対象の情報処理装置にある関連付け情報106、インストール情報105、オブジェクト共有情報109を読み出してポリシー設定支援ツール1200へ送信し、ポリシー設定支援ツール1200からは作成したポリシー情報1310を上記代理プログラムに返信してポリシーファイル1220に格納すればよい。

なお、上記各実施形態において、情報処理装置とサーバにて実行される各プログラムは、予め各装置の記憶装置に格納されていてもよいし、図示していない着脱可能な記憶媒体または通信媒体（すなわちネットワークまたはネットワークを伝搬する搬送波）を介して、上記記憶部に導入されてもよい。

The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense. It will, however, be evident that various modifications and changes may be made thereto without departing from the spirit and scope of the invention as set forth in the claims.

## WE CLAIM

### 請求項 1

コンピュータが管理する資産をポリシー情報に基づいてアクセス制御するアクセス制御部を備えたコンピュータシステムにおいて、前記ポリシー情報を作成するためのポリシー設定支援ツールであって、

前記サブジェクトの種類毎に用意した情報とは、サブジェクトの種類毎に標準的あるいは推奨のポリシーを記述したサンプル情報と、サブジェクトの正常な動作を記録したアクセスログ情報と、対象のコンピュータシステムにインストールされているサブジェクトのインストール先パス名を含むインストール情報とからなり、

前記オブジェクトの種類毎に用意した情報とは、オブジェクトの種類毎にアクセス手段として利用される頻度の高いサブジェクトの情報を記述した関連付け情報とからなり、

前記ポリシー設定支援ツールは、

前記サブジェクトの動作を監視して前記アクセスログ情報に記録するためのアクセス監視部と、

前記サンプル情報と前記インストール情報とを照合して差分を検出する差分検出部と、

前記サンプル情報と前記関連付け情報と前記差分検出部による検出結果とからポリシーの原案を作成するポリシー生成部と、

ポリシーの原案を表示して利用者による更なるポリシーの修正および保存をするためのユーザインタフェース部とから構成される。

### 請求項 2

請求項 1 記載のポリシー設定支援ツールであって、

前記ユーザインタフェース部を通じて、ユーザの操作に従い、前記サンプル情報と、前記関連付け情報と、前記アクセスログ情報とから、1つ以上の情報を用いてポリシーの原案を作成する手段と、

当該ポリシー原案への修正操作を受け付け、修正後のポリシーを保存することで、前記ポリシー情報を設定する手段を備える。

### 請求項 3

コンピュータが管理する資産をポリシー情報に基づいてアクセス制御するアクセス制御部を備えたコンピュータシステムにおいて、前記ポリシー情報を維持するためのポリシー設定支援ツールであって、

アクセス対象となるオブジェクトならびにアクセス主体となるサブジェクトに関する最新情報と、当該最新情報と設定済みのポリシーの内容とを照合しながら更新すべき項目を検出するための差分検出部と、

当該差分検出部による検出結果からポリシーの原案を作成するポリシー生成部と、

ポリシーの原案を表示して利用者による目視確認および前記ポリシーの更新処理をするためのユーザインタフェース部とから構成される。

#### 請求項4

請求項3記載のポリシー設定支援ツールであって、

前記差分検出部による検出処理は、定期的に、あるいは利用者からの要求を受けた時点で実行されるものであり、差分を検出した場合には、当該差分情報を、前記ユーザインタフェース部を通じて利用者向けに表示し、

前記ポリシー設定支援ツールの利用者は、前記ユーザインタフェース部を通じて表示される前記差分情報を目視で確認し、当該表示通りに更新すべきかどうかを判断し、更新すべきであれば前記ユーザインタフェース部を通じて必要な修正を加えた上で、前記ポリシー情報を保存することを特徴とする。

#### 請求項5

コンピュータが管理する資産をポリシー情報に基づいてアクセス制御するアクセス制御部を備えたコンピュータシステムにおいて、前記ポリシー情報を作成するためのポリシー設定支援ツールであって、

アクセス対象となるオブジェクトの種類毎にアクセス手段として利用される頻度の高いサブジェクトの情報を記述した関連付け情報を備え、

当該関連付け情報からポリシー情報を作成する手段を備える。

#### 請求項6

請求項5記載のポリシー設定支援ツールであって、

前記ポリシー設定支援ツールは、オブジェクトへのアクセス手段を用途別に指定するための用途別サブジェクト指定手段を備えており、

当該用途別サブジェクト指定手段を利用して指定されたプログラムを、複数種類のオブジェクトにアクセス可能なサブジェクトとして前記ポリシー情報を作成する手段を備える。

#### 請求項7

請求項5記載のポリシー設定支援ツールであって、

前記コンピュータシステムは、複数のサブジェクト間でオブジェクトを共有するためのオブジェクト共有処理部を備えたサブジェクトの識別子一覧と、当該サブジェクトから利用可能なオブジェクトの種類とを記述したオブジェクト共有情報を備えており、

前記ポリシー設定支援ツールは、前記オブジェクト共有情報に登録されたサブジェクトに対して、当該サブジェクトから利用可能なオブジェクトへのアクセスを全て許可、または一部許可するポリシー情報を作成する手段を備える。



#### 請求項 8

請求項 5 記載のポリシー設定支援ツールであって、

前記ポリシー設定支援ツールは、前記ポリシー情報に違反するアクセスが発生した場合に前記アクセス制御部から通知を受けて、当該アクセスの対象となるオブジェクトを管理するコンピュータシステムの利用者に対してメッセージを伝え、前記利用者による判断に基づいて所定の処理を実行する手段を備えており、

前記利用者による判断とは、前記ポリシー違反のアクセスを以後全て許可するか、今回のアクセスのみ許可するか、禁止するかのいずれかであり、

前記ポリシー違反のアクセスを以後全て許可する場合には、前記ポリシー設定支援ツールによる所定の処理として前記アクセスが正当なアクセスとなるようポリシー情報を変更し、前記アクセス制御部に対しては前記アクセスが正当であることを通知し、

前記ポリシー違反のアクセスを今回のみ許可する場合には、所定の処理として前記ポリシー情報は変更せずに、前記アクセス制御部に対しては前記アクセスが正当であることを通知し、

前記ポリシー違反のアクセスを禁止する場合には、所定の処理として前記ポリシー情報は変更せず、前記アクセス制御部に対しては前記アクセスが不正であることを通知する。

#### 請求項 9

請求項 5 記載のポリシー設定支援ツールであって、

前記ポリシー設定支援ツールは、前記ポリシー情報に登録されていないオブジェクトに対して、当該オブジェクトに関連付けられたサブジェクトからアクセスが発生した時に、前記アクセス制御部から通知を受け、前記コンピュータシステムの利用者に対してメッセージを伝え、前記利用者による判断に基づいて所定の処理を実行する手段を備えており、

前記利用者による判断とは、前記登録されていないオブジェクトに対する当該オブジェクトに関連付けられたサブジェクトからのアクセスを許可するか、禁止するかのいずれかであり、

前記アクセスを許可する場合には、前記ポリシー設定支援ツールによる所定の処理として前記アクセスが正当なアクセスとなるようポリシー情報を変更して、前記アクセス制御部に対しては前記アクセスが正当であることを通知し、

前記アクセスを禁止する場合には、前記ポリシー情報は変更せず、前記アクセス制御部に対しては前記アクセスが不正であることを通知する。

#### 請求項 10

請求項 5 記載のポリシー設定支援ツールであって、

前記ポリシー設定支援ツールは、前記ポリシー情報に登録された情報とは一部異なるサ

ブジェクトからアクセスが発生した時に、前記アクセス制御部から通知を受け、前記コンピュータシステムの利用者に対してメッセージを伝え、前記利用者による判断に基づいて所定の処理を実行する手段を備えており、

前記利用者による判断とは、前記サブジェクトからのアクセスを許可するか、禁止するかのいずれかであり、

前記アクセスを許可する場合には、前記ポリシー設定支援ツールによる所定の処理として前記サブジェクトが正当なものとなるようポリシー情報を変更して、前記アクセス制御部に対しては前記アクセスが正当であることを通知し、

前記アクセスを禁止する場合には、前記ポリシー情報を変更せず、前記アクセス制御部に対しては前記アクセスが不正であることを通知する。

## ABSTRACT

本発明が提供するポリシー設定支援ツールは、ソフトウェアの種類毎のポリシーを記述したサンプル情報と、オブジェクトの種類毎に利用頻度の高いプログラムの情報を記述した関連付け情報と、プログラムの動作を監視して記録したアクセスログ情報のいずれかを用いてポリシーの原案を作成するポリシー生成部１０２と、ポリシー原案を表示して、利用者による確認と編集を可能とするユーザインタフェース部１０１の処理により、適切なポリシー設定に必要な作業の簡易化を実現する。また差分検出部１０４により、設定済みポリシーから更新すべき部分を、現在のオブジェクト１１２とサブジェクト情報１１３を参照して検出し、ユーザインタフェース部１０１を通じて提示するとともに、簡易に更新可能とすることで、適切なポリシー維持も可能とする。